IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Ex Parte:	ANDERSON, WALTER
Application Number:	09/938,184
Filing Date:	August 23, 2001
Title:	Key Management Methods for Secure Communication Systems
Group:	2137
Examiner:	KEVIN R. SCHUBERT

BRIEF ON BEHALF OF APPELLANTS UNDER 37 CFR 41.37

Valerie M. Davis
Attorney of Record

Motorola, Inc.
Intellectual Property Section
Law Department
1303 E. Algonquin Rd.
Schaumburg, IL 60196

Telephone: 847-576-6733
Facsimile: 847-576-0721

Submittal Date: December 30, 2006

CONTENTS

I. REAL PARTY IN INTEREST

The name of the real party in interest for purposes of this appeal is Motorola, Inc., a Delaware corporation.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to the Applicant, the Applicant's legal representative, or assignee which would directly affect or be directly affected by or having a bearing on the Board's decision in this pending appeal.

III. STATUS OF CLAIMS

Claims 12-18 remain in the application. Claims 12-18 are being appealed. Claims 12-18 stand or fall together.

In a final Office Action dated August 23, 2006, the Examiner rejected Claims 12-13 under 35 U.S.C. 102(b) as being anticipated by Gardeck, et al. (USPN 5,471,532); Claim 14 under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Doiron (USPN 5,481,610); Claim 15 under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Miller (USPN 6,208,612); and Claims 16-18 under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Schneier (Schneier, Bruce, Applied Cryptography, CRC Press, 1996, pages 1-2) .

IV. STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the Final Office Action mailed August 23, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Although specification citations are inserted below in accordance with 37 C.F.R. § 41.37, these reference numerals and citations are merely examples of where support may be found in the specification for the terms used in this section of the brief. There is no intention to in any way suggest that the terms of the claims are limited to the examples in the specification. Although, as demonstrated by the reference numerals and citations below, the claims are fully supported by the specification as required by law, it is improper under the law to read limitations from the specification into the claims. Pointing out specification support for the claim terminology, as is done here to comply with rule 41.37, does not in any way limit the scope of the claims to those examples from which they find support. Nor does this exercise provide a mechanism for circumventing the law precluding reading limitations into the claims from the specification. In short, the reference numerals and specification citations are not to be construed as claim limitations or in any way used to limit the scope of the claims.

The invention, as defined in independent Claims 1 and with reference to FIGs. 1, 3 and 4, is a communication system including a centralized key management facility (403), a manual key delivery device (101) and a number of encryption devices (103), a method comprising the steps of: receiving (305), by a manual key delivery device from a centralized key management facility that is remote from the manual key delivery device, one or more key management messages including indicia of respective target communication devices that are to receive the key management messages; operably connecting (310) the key delivery device to one or more candidate encryption devices; determining (315), by the key delivery device upon connecting to the one or more candidate encryption devices and based on the indicia included in the one or

more received key management messages, which ones of the candidate encryption devices are target encryption devices; and delivering (325), from the key delivery device, one or more key management messages to the candidate encryption devices determined by the key delivery device to be target encryption devices. (Specification page 11, line 22 to page 12, line 29).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether Claims 12-13 are patentable under 35 U.S.C. 102(b) over Gardeck, et al.?

B. Whether Claim 14 is patentable under 35 U.S.C. 103(a) over Gardeck, et al. in view of Doiron?

C. Whether Claim 15 is patentable under 35 U.S.C. 103(a) over Gardeck, et al. in view of Miller (USPN 6,208,612)?

D. Whether Claims 16-18 are patentable under 35 U.S.C. 103(a) over Gardeck, et al. in view of Schneier (Schneier, Bruce, Applied Cryptography, CRC Press, 1996, pages 1-2)?

VII. ARGUMENT

A. Claims 12-13 are rejected under 35 U.S.C. 102(b) as being anticipated by Gardeck, et al. (USPN 5,471,532).

MPEP § 2131 provides:

> A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F. 2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as

> complete detail as contained in the … claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim ….

Regarding Claims 12-13, the Examiner asserts that Gardeck, et al. anticipates (i.e., discloses all elements of) Appellants' claimed invention (Office Action, August 23, 2006, pages 2-3). It is noted that the Examiner's reliance upon Gardeck, et al., et al. appears to be misplaced.

Gardeck, et al. discloses the use of multiple Key Management Controllers (illustrated as a home key unit, a first key unit and a second key unit) to send updated key information to roaming communication units. The patent is very clear that "the present invention provides for a method for *over-the-air rekeying* of roaming communication units" (Abstract; col. 1, lines 61-61). No manual key delivery device is used in the Gardeck, et al. reference to update the communication units. Only the key units are used to send the updated key information, and these key units are all centralized key management controllers or KMCs, which assign a key by over-the-air rekeying. Col. 1, lines 19-22; col. 2, lines 19-21.

Thus, Gardeck, et al. fails to disclose the limitations recited in Claim 12 and included by dependency in Claim 13 of "*receiving by a manual key delivery device* from a centralized key management facility that is remote from the manual key delivery device, one or more key management messages including indicia of respective target communication devices that are to receive the key management messages; *operably connecting the key delivery device* to one or more candidate encryption devices; *determining, by the key delivery device* upon connecting to the one or more candidate encryption devices and based on the indicia included in the one or more received key management messages, which ones of the candidate encryption devices are target encryption devices; and *delivering, from the key delivery device*, one or more key

management messages to the candidate encryption devices determined by the key delivery device to be target encryption devices."

Therefore, since limitations are missing from the Gardeck, et al. reference, a rejection of Claims 12-13 under 35 U.S.C. § 102(b) is improper and should be withdrawn.

B. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Doiron (USPN 5,481,610).

To establish a *prima facie* case of obviousness, and hence to find Claim 14 unpatentable under 35 U.S.C. § 103(a) over the combination of Gardeck, et al. and Doiron, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not be based upon applicant's disclosure. MPEP at § 2142.

In the present case, all three criteria are not met because the combined teachings of the Gardeck, et al. and Doiron references do not teach or suggest all of the claim limitations of Claim 14. Applicants have set forth limitations that are recited in Claim 12 and included by dependency in Claim 14, which are not disclosed in Gardeck, et al. Applicants further submit that these limitations are also not disclosed in Doiron. Therefore, since limitations are missing from the Gardeck, et al. and Doiron references, a rejection of Claim 14 under 35 U.S.C. § 103(a) is improper and should be withdrawn.

C. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Miller (USPN 6,208,612)

The Examiner has not established a *prima facie* case of obviousness with respect to Claim 15 since the combined teachings of the Gardeck, et al. and Miller references do not teach or suggest all of the claim limitations of Claim 15. Applicants have set forth limitations that are recited in Claim 12 and included by dependency in Claim 15, which are not disclosed in Gardeck, et al. Applicants further submit that these limitations are also not disclosed in Miller. Therefore, since limitations are missing from the Gardeck, et al. and Miller references, a rejection of Claim 15 under 35 U.S.C. § 103(a) is improper and should be withdrawn.

D. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gardeck, et al. in view of Schneier (Schneier, Bruce, Applied Cryptography, CRC Press, 1996, pages 1-2).

The Examiner has not established a *prima facie* case of obviousness with respect to Claims 16-18 since the combined teachings of the Gardeck, et al. and Schneier references do not teach or suggest all of the claim limitations of Claims 16-18. Applicants have set forth limitations that are recited in Claim 12 and included by dependency in Claims 16-18, which are not disclosed in Gardeck, et al. Applicants further submit that these limitations are also not disclosed in Schneier. Therefore, since limitations are missing from the Gardeck, et al. and Schneier references, a rejection of Claims 16-18 under 35 U.S.C. § 103(a) is improper and should be withdrawn.

For the reasons set forth above, Applicants submit that the Examiner has incorrectly rejected Claims 12-13 under 35 U.S.C. § 102(b) and Claims 14-18 under 35 U.S.C. § 103(a) and request that the Board withdraw the rejections.

Respectfully submitted,

Anderson, et al.

by: /Valerie M. Davis/
Valerie M. Davis
Attorney for Applicant
Registration No. 50,203
Phone: (847) 576-6733
Fax: (847) 576-0721

VIII. CLAIMS APPENDIX

1-11 (withdrawn)

12. (previously presented) In a communication system including a centralized key management facility, a manual key delivery device and a number of encryption devices, a method comprising the steps of:

receiving, by a manual key delivery device from a centralized key management facility that is remote from the manual key delivery device, one or more key management messages including indicia of respective target communication devices that are to receive the key management messages;

operably connecting the key delivery device to one or more candidate encryption devices;

determining, by the key delivery device upon connecting to the one or more candidate encryption devices and based on the indicia included in the one or more received key management messages, which ones of the candidate encryption devices are target encryption devices; and

delivering, from the key delivery device, one or more key management messages to the candidate encryption devices determined by the key delivery device to be target encryption devices.

13. (original) The method of claim 12 further comprising the steps of:

determining, by the key delivery device upon connecting to the one or more candidate encryption devices, which ones of the candidate encryption devices are not target encryption devices; and

not delivering key management messages to the candidate encryption devices determined by the key delivery device not to be target encryption devices.

14. (original) The method of claim 12 further comprising the step of displaying, by the key delivery device upon a successful delivery of a key management message to a target encryption device, a message indicative of the successful delivery of the key management message to the target encryption device.

15. (original) The method of claim 12 further comprising the step of displaying, by the key delivery device upon an unsuccessful delivery of a key management message to a target encryption device, a message indicative of the unsuccessful delivery of a key management message to the target encryption device.

16. (original) The method of claim 12, wherein the step of receiving one or more key management messages comprises receiving an encrypted key management message to be delivered in red transfer to target mode, the method comprising:

decrypting the encrypted key management message, yielding an unencrypted key management message including a target destination identifier; and

delivering the unencrypted key management message to a target communication device corresponding to the target destination identifier.

17. (original) The method of claim 12, wherein the step of receiving one or more key management messages comprises receiving an encrypted key management message to be delivered in black transfer to target mode, the method comprising:

determining a target destination identifier associated with the encrypted key management message; and

delivering the encrypted key management message to a target communication device corresponding to the target destination identifier.

18. (original) The method of claim 17, wherein the step of receiving an encrypted key management message comprises receiving a key management message frame including a key management message field and a target destination field, the key management message field including the encrypted key management message and the target destination field including an encrypted target destination identifier, the step of determining a target destination identifier being accomplished by decrypting the encrypted target destination identifier.

IX. EVIDENCE APPENDIX

No evidence has been submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, entered by the examiner and relied upon by the appellant in the appeal, or relied upon by the examiner as to grounds of rejection to be reviewed on appeal.

X. RELATED PROCEEDINGS APPENDIX

No decisions have been rendered by a court of the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 C.F.R. § 41.37.